EV550715454

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Veröffentlichungsnummer: **0 616 429 A1**

(12) EUROPÄISCHE PATENTANMELDUNG

(21) Anmeldenummer: **94100237.0**

(22) Anmeldetag: **10.01.94**

(51) Int. Cl.[5]: **H03K 3/84**, G06F 7/58, H04L 9/22

(30) Priorität: **19.01.93 DE 4301279**

(43) Veröffentlichungstag der Anmeldung:
21.09.94 Patentblatt 94/38

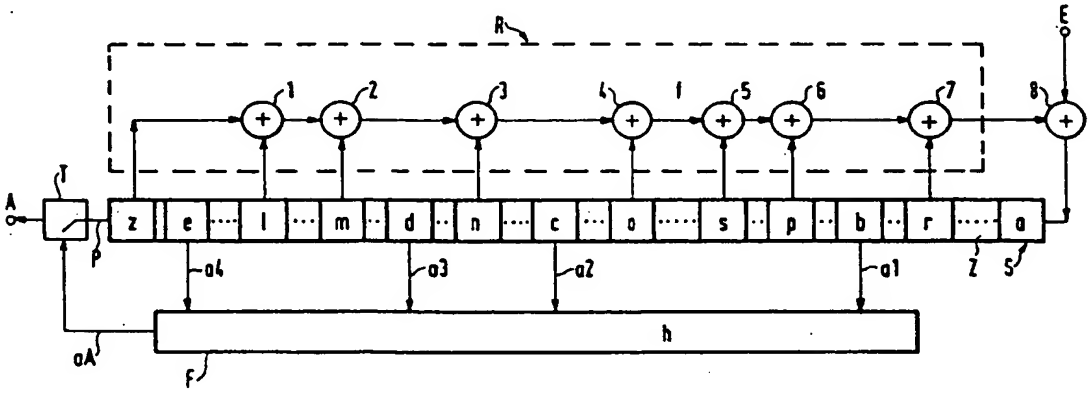
(84) Benannte Vertragsstaaten:
DE FR GB GR IT

(71) Anmelder: **SIEMENS AKTIENGESELLSCHAFT**
Wittelsbacherplatz 2
D-80333 München (DE)

(72) Erfinder: **Hess, Erwin, Dr. rer. nat.**
Meisenstrasse 18
D-85521 Ottobrunn (DE)
Erfinder: **Schrenk, Hartmut, Dr. rer. nat.**
Fasanenweg 22
D-85540 Haar (DE)
Erfinder: **Eberhard, Günther, Dipl.-Phys.**
Herbststrasse 45
D-82223 Eichenau (DE)
Erfinder: **Rueppel, Rainer, Dr.**
Bahnhofstrasse 242
CH-8623 Wetzikon (CH)

(54) Verfahren und Schaltungsanordnung zum Erzeugen einer Pseudozufallsfolge sowie deren Verwendung.

(57) Die Erfindung schlägt ein Verfahren und eine Schaltungsanordnung zur Durchführung des Verfahrens vor, um eine Pseudozufallsfolge von Bitdaten unter Verwendung einer rückgekoppelten Schieberegistereinrichtung zu erzeugen, wobei mindestens ein Schaltzustand der Schieberegistereinrichtung festlegt, ob eine Ausgabe der Bitdaten erfolgt. Ein solches Verfahren bzw. eine Schaltungsanordnung zur Durchführung des Verfahrens wird bevorzugt zur Verschlüsselung von Daten, insbesondere zur Echtheitserkennung einer Datenträgeranordnung, beispielsweise einer Chipkarte, verwendet.



$$h = X_e \cdot X_d \cdot X_e \cdot X_c \cdot X_e \cdot X_b \cdot X_d \cdot X_c \cdot X_d \cdot X_b$$

EP 0 616 429 A1

BNSDOCID: <EP___0616429A1_I_>

Best Available Copy

Die Erfindung betrifft ein Verfahren und eine Schaltungsanordnung zum Erzeugen einer Pseudozufallsfolge von Bitdaten unter Verwendung einer rückgekoppelten Schieberegistereinrichtung.

Pseudozufallsfolgen bzw. pseudozufällige Binärfolgen werden vielfach zur Untersuchung von analogen und digitalen Systemen eingesetzt. Darüber hinaus spielen Pseudozufallsfolgen eine bedeutende Rolle bei der Verschlüsselung von Daten.

Es sind zahlreiche Schaltungsanordnungen bekannt, solche Pseudozufallsfolgen von Bitdaten zu erzeugen. In dem Buch Tietze, Schenk "Halbeiter-Schaltungstechnik", 5. Auflage sind auf den Seiten 509 bis 512 Schaltungsanordnungen beschrieben, um solche Pseudozufallsfolgen zu erzeugen. Zur Erzeugung von Pseudozufallsfolgen verwendet man üblicherweise Schieberegister, die in bestimmter Weise rückgekoppelt sind. Die Rückkopplung wird dabei aus Exklusiv-ODER-Schaltungen zusammengesetzt. Die größte nicht periodische Bitfolge, die ein Schieberegister mit n Stufen erzeugen kann, ist $N = 2^n-1$ Bit lang. So kann mit einem vierstufigen Schieberegister beispielsweise eine Pseudozufallsfolge mit einer maximalen Periodenlänge von 15 Bit erzeugt werden. Eine dafür geeignete Schaltung ist in Abbildung 20.23 der genannten Literaturstelle zu sehen.

Beim Verschlüsseln von Daten wird dagegen die rückgekoppelte Schieberegistereinrichtung mit einer Schlüsselinformation, d.h. ein geheimes Datenwort, beaufschlagt. Mit diesem Datenwort wird festgelegt, an welcher Stelle der Pseudozufallsfolge am Ausgang der rückgekoppelten Schieberegistereinrichtung der Datenstrom der Pseudozufallsfolge beginnt.

Befindet sich beispielsweise in einer tragbaren Datenträgeranordnung, wie z.B. einer Chipkarte, und in einer mit dieser zusammenarbeitenden Datenein-/ausgabeeinrichtung jeweils ein gleiches rückgekoppeltes Schieberegister, und ist der gleiche Schlüssel auf beiden Seiten bekannt, so können die von der einen Datenträgeranordnung zur Datenein/ausgabeeinrichtung verschlüsselt gesendeten Daten wieder entschlüsselt bzw. ein zwischen beiden Seiten ausgetauschter Datenstrom gleichermaßen verschlüsselt und die verschlüsselten Daten verglichen werden. Damit ist unter anderem ein Echheitsnachweis der Chipkarte möglich und ein gewisser Schutz vor Fälschungen bzw. Mißbrauch sichergestellt.

Bisherige Verfahren und Konzepte zur Sicherung solcher Datenträgeranordnung verwenden anstelle einer strengen Echtheitsprüfung zur Ausschaltung von Fälschungen und Mißbrauch die Überprüfung eines durch Nachbauten oder Emulationen nur sehr schwer realisierbaren charakteristischen Merkmals. Bekannt ist darüber hinaus auch die Überprüfung der Gültigkeit der gespeicherten Daten über den Zusatz eines mit dem oben bereits erwähnten geheimen Schlüssel in einer Datenträgeranordnung erzeugten Codes für einen Echtheitsnachweis des Dateninhalts.

Problematisch ist bei diesem bekannten Verfahren, daß die Kontrollsignale abgehört bzw. am Ein/Ausgang der Datenträgeranordnung, beispielsweise der Chipkarte, abgegriffen werden können, wodurch ein Wiedereinspielen der Kontrollinformation zur Fälschungszwecken möglich ist.

Bei elektronischen Schaltungen mit Mikroprozessorarchitektur wird dieser Nachteil durch Einsatz eines kryptografischen Authentifikations- oder Identifikationsvorganges nach dem Prinzip der herausfordernden Frage und dazu passenden Antwort (Challenge und Response-Prinzip) bzw. mit Zero-Knowledge-Protokoll ausgeschaltet.

Dieses Challenge-Response-Prinzip sieht beispielsweise bei einer Chipkarte und einer Datenein-/ausgabeeinrichtung zum Lesen dieser Chipkarte vor, daß zunächst die Datenein-/ausgabeeinrichtung Daten "Challenge" generiert und diese zur Chipkarte sendet. Dort dient diese "Challenge" zur Berechnung einer sogenannten "Response". Diese "Response" wird mittels eines Algorithmusses zum Echtheitsnachweis berechnet und hängt zweckmäßigerweise von weiteren Daten, dem geheimen Kartenschlüssel und z.B. einer weiteren Größe, wie einem internen Zählerstand, ab. Die von der Chipkarte zur Datenein-/ausgabeeinrichtung gesendete "Response" wird in der Datenein-/ausgabeeinrichtung mit dort vorliegenden Daten verglichen. Diese dort vorliegenden Daten werden mit dem gleichen Algorithmus, dem gleichen geheimen Kartenschlüssel, der Challenge und der Zusatzinformation berechnet. Stimmt die Response mit dieser Berechnung überein, so ist die Chipkarte als gültig erkannt. Andernfalls erfolgt ein Abbruch der Datenverbindung zwischen Chipkarte und Datenein-/ausgabeinrichtung.

Die eingangs erwähnte rückgekoppelte Schieberegistereinrichtung wird bei diesen bekannten Systemen dazu verwendet, den geheimzuhaltenden Kartenschlüssel in eine längere Pseudozufallsfolge, eine sogenannte Schlüsselstromfolge, zu transformieren. Bei Vorgabe beliebiger Teile der Schlüsselstromfolge muß es einem Angreifer, der den Kartenschlüssel unbefugter Weise berechnen will, unmöglich sein, weitere Teile der Schlüsselstromfolge vorherzusagen. Dies impliziert, daß es ebenfalls unmöglich sein muß, auf den Schlüssel zurückzurechnen. Die bisher bekannten rückgekoppelten Schieberegistereinrichtungen gewähren hierfür bereits einen guten Schutz, sofern die Schieberegistereinrichtung hinreichend lang ist, z.B. 50 hintereinander geschaltete Schieberegisterzellen aufweist. Es besteht jedoch ein Bestreben dahin, diese bekannten Verfahren mit geringstmöglichen Auf-

BNSDOCID: <EP___0616429A1_I_>

Best Available Copy

wand noch besser zu sichern. Hier setzt die Erfindung an.

Der Erfindung liegt die Aufgabe zugrunde, ein Verfahren zum Erzeugen einer Pseudozufallsfolge von Bitdaten unter Verwendung einer rückgekoppelten Schieberegistereinrichtung sowie eine Schaltungsanordnung zur Durchführung des Verfahrens anzugeben, das gegenüber dem bisher bekannten Verfahren und Schaltungsanordnungen eine höhere Sicherheit aufweist. Darüber hinaus soll eine geeignete Verwendung für dieses Verfahren und diese Schaltungsanordnung aufgezeigt werden.

Diese Aufgabe wird für ein Verfahren zum Erzeugen einer Pseudozufallsfolge von Bitdaten unter Verwendung einer rückgekoppelten Schieberegistereinrichtung dadurch gelöst, daß mindestens ein Schaltzustand der Schieberegistereinrichtung festlegt, ob eine Ausgabe der Bitdaten erfolgt.

In eine Weiterbildung des erfindungsgemäßen Verfahrens ist es vorgesehen, daß Ausgangssignale einzelner Schieberegisterzellen der Schieberegistereinrichtung einer nichtlinearen logischen Funktion als Eingangsvariable zugeführt werden und ein logisches Ausgangssignal der nichtlinearen logischen Funktion die Ausgabe der Bitdaten steuert.

Die Aufgabe wird für eine Schaltungsanordnung zur Durchführung des Verfahrens dadurch gelöst, daß eine ausgangsseitig eine Schalteinrichtung aufweisende rückgekoppelte Schieberegistereinrichtung mit einer Vielzahl hintereinander geschalteter Schieberegisterzellen vorgesehen ist, und daß eine vorgegebene Anzahl von Schieberegisterzellen ausgangsseitig mit einer eine nichtlineare logische Funktion realisierenden Schaltung verbunden ist, welche ausgangsseitig mit der Schalteinrichtung zu deren Steuerung in Verbindung steht.

In einer vorteilhaften Weiterbildung der erfindungsgemäßen Schaltungsanordnung ist vorgesehen, daß die eine nichtlineare logische Funktion realisierende Schaltung logische UND- und logische ODER-Gatter aufweist. Darüber hinaus kann die Schalteinrichtung selbst ein logisches Gatter, beispielsweise ein UND-Gatter sein, das an einer ersten Eingangsklemme mit einem Ausgang der Schieberegistereinrichtung und mit einer Eingangsklemme mit einer Ausgangsklemme der die nichtlineare logische Funktion realisierenden Schaltung verbunden ist. Am Ausgang dieses UND-Gatters ist dann die Pseudozufallsfolge abgreifbar. Je nachdem, ob die Schalteinrichtung ein- oder ausgeschaltet ist, gelangen demnach die von der rückgekoppelten Schieberegistereinrichtung erzeugten Bitdaten an den Ausgang der erfindungsgemäßen Schaltungsanordnung. So lange die Schalteinrichtung ausgeschaltet ist, gelangen dagegen keine Daten an die Ausgangsklemme der erfindungsgemäßen Schaltungsanordnung. Um eine solche Datenlücke zu vermeiden, kann vorgesehen werden, daß ausgangsseitig an die erfindungsgemäße Schaltungsanordnung ein Zwischenspeicher geschaltet wird, welches mit fortlaufendem Takt ausgelesen wird.

Gemäß der Erfindung wird das Verfahren oder die Schaltungsanordnung zur Verschlüsselung bzw. Entschlüsselung von Daten und/oder in einer Datenträgeranordnung, insbesondere Chipkarten mit integrierten Schaltungsanordnungen, zu deren Echtheitserkennung eingesetzt.

Die Erfindung wird im folgenden anhand eines Ausführungsbeispieles in Zusammenhang mit einer Figur näher erläutert.

Die erfindungsgemäße Schaltungsanordnung sieht eine rückgekoppelte Schieberegistereinrichtung vor, welche eine Vielzahl von hintereinander geschaltete Schieberegisterzeilen a...z aufweist. Die eingangsseitige Schieberegisterzelle ist mit dem Bezugszeichen a und die ausgangsseitige Schieberegisterzelle mit dem Bezugszeichen z bezeichnet. Diese hintereinander geschalteten Schieberegisterzellen a...z sind über eine EXOR-Gatter 1 bis 7 enthaltene Rückkopplungsschaltung R rückgekoppelt. Hierfür sind in dem in der Figur 1 gezeigten Ausführungsbeispiel sieben EXOR-Gatter 1 bis 7 in der Rückkopplungseinrichtung R vorgesehen. Diese EXOR-Gatter 1 bis 7 weisen jeweils zwei Eingangsklemmen und eine Ausgangsklemme auf, wobei ein erstes EXOR-Gatter 1 mit einem Ausgangssignal der letzten Schieberegisterzelle z und mit einem Ausgangssignal der Schieberegisterzelle 1 beaufschlagt ist. Die Ausgangsklemme des EXOR-Gatters 1 ist mit einer Eingangsklemme des zweiten EXOR-Gatters 2 in Verbindung, deren andere Eingangsklemme an den Ausgang einer mit m bezeichneten Schieberegisterzelle verbunden ist. In dem in der Figur dargestellten Ausführungsbeispiel sind die weiteren EXOR-Gatter 3, 4, 5, 6 und 7 derart verschaltet, daß dem EXOR-Gatter 3 das Ausgangssignal des EXOR-Gatters 2 und das Ausgangssignal einer Schieberegisterzelle n, dem EXOR-Gatter 4 das Ausgangssignal des EXOR-Gatters 3 und ein Ausgangssignal einer Schieberegisterzelle o, das Ausgangssignal des EXOR-Gatters 4 und ein Ausgangssignal der Schieberegisterzelle s dem EXOR-Gatter 5 zugeführt wird, daß das Ausgangssignal des EXOR-Gatters 5 und ein Ausgangssignal der mit p bezeichneten Schieberegisterzelle dem EXOR-Gatter 6 zugeleitet wird, und dessen Ausgangssignal und ein Ausgangssignal einer Schieberegisterzelle r dem EXOR-Gatter 7 zugeführt wird. Das mit dem Bezugszeichen 8 bezeichnete EXOR-Gatter erhält einerseits das Ausgangssignal des EXOR-Gatter 7 und andererseits ein Eingangssignal E, das unter anderem den geheimzuhaltenden Schlüssel repräsentiert. Ausgangsseitig ist dieses EXOR-Gatter 8 mit einem

BNSDOCID: <EP__0616429A1_I_>

Best Available Copy

Eingang der ersten Schieberegisterzelle a der Schieberegistereinrichtung verbunden.

Dieses Eingangssignal E kann beispielsweise aus einer Geheiminformation, einer Zufallszahl als Challenge und gegebenenfalls einer Zusatzinformation (z.B. ein Datenspeicherinhalt) gewonnen werden. Die erfindungsgemäße Schaltungsanordnung ist nicht auf das in der Figur dargestellte EXOR-Gatter 8 beschränkt. Vielmehr kann dieses EXOR-Gatter 8 durch eine beliebige Verknüpfungslogik ersetzt sein.

Erfindungsgemäß ist an den Ausgang der rückgekoppelten Schieberegistereinrichtung eine Schalteinrichtung T geschaltet, die abhängig von einem Steuersignal aA die am Ausgang der letzten Schieberegisterzelle z anstehende Pseudozufallsfolge P von Bitdaten an eine Ausgangsklemme A durchschaltet oder nicht. Das Steuersignal aA wird erfindungsgemäß durch eine eine nichtlineare logische Funktion h realisierende Schaltung F erzeugt, welche in Abhängigkeit eines oder mehrerer Schaltzustände der Schieberegistereinrichtung S festlegt, ob die Schalteinrichtung T die an ihrem Eingang anstehende Pseudozufallsfolge P an die Ausgangsklemme A schaltet oder nicht. Hierfür ist die Schaltung F eingangsseitig mit Ausgängen von vorgegebenen Schieberegisterzellen verbunden. In diesem Ausführungsbeispiel ist angenommen, daß Ausgänge von vier Schieberegisterzellen nämlich der Schieberegisterzellen b, c, d und e über Verbindungsleitungen a1, a2, a3, a4 mit der Schaltung F in Verbindung stehen. Die nichtlineare logische Funktion h besteht beispielsweise aus einer Kombination von UND- und ODER-Gattern folgender Art:

$$h = X_e \cdot X_d + X_e \cdot X_c + X_e \cdot X_b + X_d \cdot X_c + X_d \cdot X_b.$$

Vorzugsweise werden die Abgriffe der die nichtlineare logische Funktion darstellenden Schaltung F an der Schieberegistereinrichtung nicht als nebeneinander liegende Blöcke gewählt. Es empfiehlt sich, diese Abgriffe zufällig und nicht übereinanderliegend zu wählen. Das gleiche gilt für die Rückkopplungsabgriffe zu den EXOR-Gattern 1 bis 7.

Die Arbeitsweise dieser erfindungsgemäßen Schaltungsanordnung ist folgende. Nach einer definierten Voreinstellung des Schieberegisterzustandes wird das Eingangssignal E, welches wie bereits erwähnt aus einer Geheiminformation, einer Zufallszahl und gegebenenfalls einer Zufallsinformation bestehen kann, in die rückgekoppelte Schieberegistereinrichtung S eingegeben. Diese Eingabe wird über eine Verknüpfungslogik, hier das EXOR-Gatter 8 mit der Rückkopplungsinformation am Ausgang des letzten EXOR-Gatters 7 verknüpft. Die Ausgabe eines Datenwortes zur Echtheitserkennung an der Ausgangsklemme A der erfindungsgemäßen Schaltungsanordnung wird durch die nichtlineare logische Funktion h der Schaltung F gesteuert. Diese wird aus der laufenden Pseudozufallsfolge P am Ausgang der letzten Schieberegisterzelle z ausgeblendet. Eine überprüfende Stelle kann dann in Kenntnis der Information E, d.h. also der Geheiminformation, der Zufallszahl und der gegebenenfalls vorhanden Zusatzinformation den gleichen Vorgang nachvollziehen. Bei Gleichheit ist die Echtheit festgestellt.

Die definierte Voreinstellung der Schieberegistereinrichtung S kann beispielsweise mit Unterbrechung der Rückkopplung über die Eingabe des Eingangssignales E, vorzugsweise der Geheiminformation erfolgen. Die Reihenfolge der Eingabe nach einer Voreinstellung kann beliebig erfolgen. Die Sperrung der Ausgabe ist erfindungsgemäß zweckmäßigerweise so gewählt, daß eine für die Sicherheit ausreichende Nichtkorrelation zur Eingabe, insbesondere der Geheimzahl, gewährleistet wird. Vor der Eingabe und/oder zwischen den Eingaben des Eingangssignales E, können mehrere Taktzyklen dazwischengeschaltet werden. Eine längere Taktzyklusphase kann darüber hinaus der eigentlichen an der Ausgangsklemme A anstehenden Pseudozufallsfolge vorgeschaltet werden.

Es hat sich als zweckmäßig erwiesen, die Ausgabe aus dem Schieberegister entsprechend der nichtlinearen Ausgabefunktion in ein Zwischenregister zu schreiben, welches mit fortlaufendem Takt ausgelesen wird. Damit ist der Vorteil ereicht, daß eine kontinuierliche Datenfolge am Ausgang der erfindungsgemäßen Schaltungsanordnung abgreifbar ist, ohne daß die sonst bei der erfindungsgemäßen Schaltungsanordnung zwangsweise sich ergebenden Datenlücken auftreten. Darüber hinaus kann die Echtheitsprüfung nach jeder Änderung des Zustandes der zu überprüfenden Schaltung wiederholt werden. Im übrigen kann die Echtheitsprüfung zwischen zwei Schaltungen gegenseitig durch Austausch entsprechender Pseudozufallsfolgen vorgesehen werden.

Mit der erfindungsgemäßen Schaltungsanordnung und dem erfindungsgemäßen Verfahren ist es also möglich, mit Hilfe der rückgekoppelten Schieberegistereinrichtung und der nichtlinearen Verknüpfungsfunktion h eine Datenfolge zu erzeugen, die aus der Pseudozufallsfolge P am Ausgang der letzten Schieberegisterzelle z der Schieberegistereinrichtung S mit Hilfe der nichtlinearen Verknüpfungsfunktion h eine weitere Zahlenfolge durch Auswahl abgeleitet wird. Für die so erzeugte Folge muß über die Wahl der Rückkopplungsfunktion und der nichtlinearen Verknüpfungsfunktion erfindungsgemäß sichergestellt sein, daß eine Voraussagbarkeit des Signales an der Ausgangsklemme A nach praktischem Ermessen unmöglich wird.

BNSDOCID: <EP___0616429A1_I_>

Best Available Copy

Patentansprüche

1. Verfahren zum Erzeugen einer Pseudozufallsfolge von Bitdaten unter Verwendung einer rückgekoppelten Schieberegistereinrichtung (R, S),
dadurch gekennzeichnet, daß mindestens ein Schaltzustand der Schieberegistereinrichtung (S, R) festlegt, ob eine Ausgabe der Bitdaten erfolgt.

2. Verfahren nach Anspruch 1,
dadurch gekennzeichnet, daß Ausgangssignale (a1, a2, a3, a4) einzelner Schieberegisterzellen (b, c, d, e) der Schieberegistereinrichtung (S, R) einer nichtlinearen logischen Funktion (h) als Eingangsvariable zugeführt werden und ein logisches Ausgangssignal (aA) der nichtlinearen Funktion (h) die Ausgabe der Bitdaten steuert.

3. Schaltungsanordnung zur Durchführung des Verfahrens nach Anspruch 1 oder 2,
dadurch gekennzeichnet, daß eine ausgangsseitig eine Schalteinrichtung (T) aufweisende rückgekoppelte Schieberegistereinrichtung (S, R) eine Vielzahl hintereinander geschalteter Schieberegisterzellen (a...z) enthält, und daß vorgegebene Schieberegisterzellen (b, c, d, e) ausgangsseitig mit einer eine nichtlineare logische Funktion (h) realisierende Schaltung (F) verbunden ist, welche ausgangsseitig mit der Schalteinrichtung (T) zu deren Steuerung in Verbindung steht.

4. Schaltungsanordnung nach Anspruch 3,
dadurch gekennzeichnet, daß die eine nichtlineare logische Funktion (h) realisierende Schaltung logische UND- und logische ODER-Gatter aufweist.

5. Schaltungsanordnung nach Anspruch 3 oder 4,
dadurch gekennzeichnet, daß die Schalteinrichtung (T) ein Logikgatter ist.

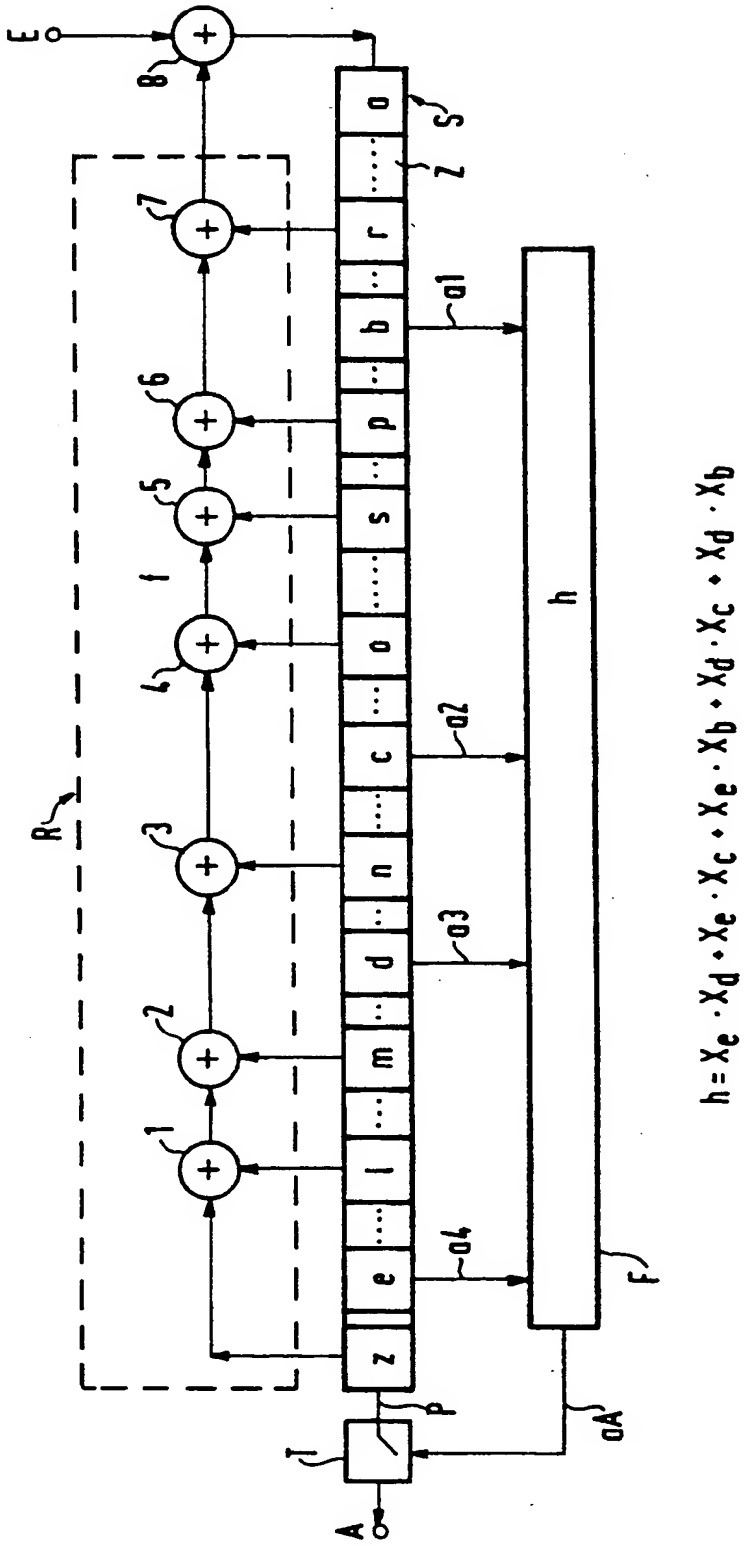
6. Schaltungsanordnung nach einem der Ansprüche 3 bis 5,
dadurch gekennzeichnet, daß an die Schalteinrichtung (T) ausgangsseitig eine Puffereinrichtung zum kontinuierlichen Ausgeben der Pseudozufallsfolge mit Daten vorgesehen ist.

7. Verwendung des Verfahrens nach Anspruch 1 oder 2 oder der Schaltungsanordnung nach einem der Ansprüche 3 bis 6 in einer Datenträgeranordnung, insbesondere einer Chipkarte mit einer integrierten Schaltungsanordnung, zur Echheitserkennung.

8. Verwendung des Verfahrens nach Anspruch 1 oder 2 oder der Schaltungsanordnung nach einem der Ansprüche 3 bis 6 zum Verschlüsseln und/oder von Daten.

3NSDOCID: <EP__0616429A1_I_>

Best Available Copy



$$h = X_e \cdot X_d + X_e \cdot X_c + X_e \cdot X_b + X_d \cdot X_c + X_d \cdot X_b$$

Best Available Copy

Europäisches Patentamt

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung
EP 94 10 0237

EINSCHLÄGIGE DOKUMENTE

Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (Int.Cl.5)
A	US-A-4 202 051 (G. I. DAVIDA ET AL.) * das ganze Dokument * ---	1,3,8	H03K3/84 G06F7/58 H04L9/22
A	ADVANCES IN CRYPTOLOGY - AUSCRYPT '90, INTERNATIONAL CONFERENCE ON CRYPTOLOGY. PROCEEDINGS, SYDNEY, NSW, AU, 8-11 JAN. 1990 Seite 32-36 GONG GUANG: 'Nonlinear generators of binary sequences with controllable complexity and double key' * Abbildung 1 * ---	1,3	
A	EP-A-0 147 716 (ANT NACHRICHTENTECHNIK GMBH) * das ganze Dokument * -----	1,3,8	

RECHERCHIERTE SACHGEBIETE (Int.Cl.5)

H03K
H04L
G06F
G06K
G07F

Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt

Recherchenort	Abschlußdatum der Recherche	Prüfer
BERLIN	5. Mai 1994	Arendt, M

KATEGORIE DER GENANNTEN DOKUMENTE

X : von besonderer Bedeutung allein betrachtet
Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie
A : technologischer Hintergrund
O : nichtschriftliche Offenbarung
P : Zwischenliteratur

T : der Erfindung zugrunde liegende Theorien oder Grundsätze
E : älteres Patentdokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist
D : in der Anmeldung angeführtes Dokument
L : aus andern Gründen angeführtes Dokument

& : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument

EPO FORM 1503 03.82 (P04C03)

BNSDOCID: <EP___0616429A1_I_>

Best Available Copy